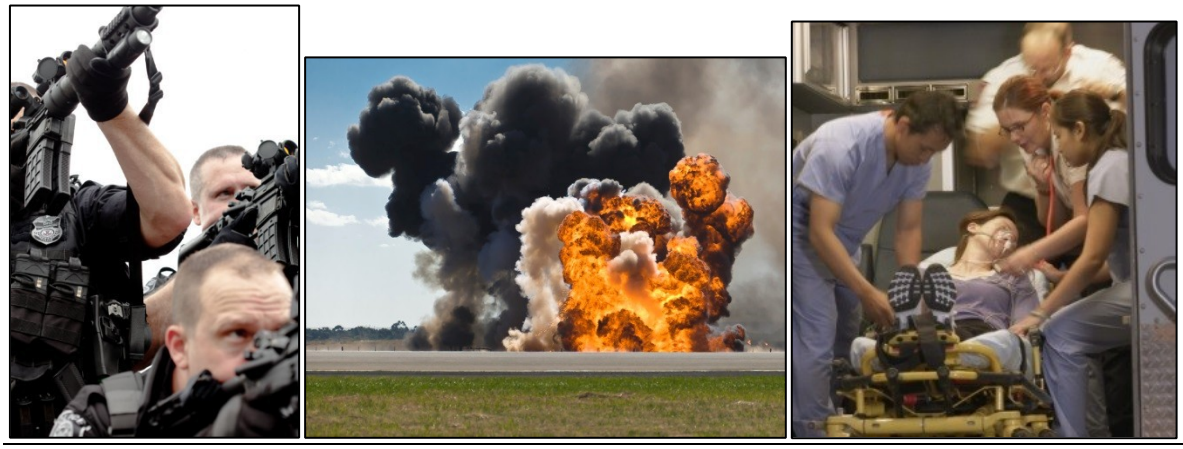

Violent Extremist Attack Tabletop Exercise

Situation Manual

[Insert Date]

[Insert Caveat]

This Situation Manual (SitMan) provides exercise participants with all the necessary tools for their roles in the exercise. Some exercise material is intended for the exclusive use of exercise planners, facilitators, and

Photo Courtesy of CISA

evaluators, but players may view other materials that are necessary to their performance. All exercise participants may view the SitMan.

This page is intentionally left blank.

Exercise Agenda

Start Time	End Time	Activity
7:45 a.m.	8:30 a.m.	Registration
8:30 a.m.	8:45 a.m.	Welcome and Participant Briefing
8:45 a.m.	9:45 a.m.	Module One: Intelligence and Information Sharing
9:45 a.m.	9:55 a.m.	Break
9:55 a.m.	10:55 a.m.	Module Two: Emergency Response
10:55 a.m.	11:05 a.m.	Break
11:05 a.m.	12:05 p.m.	Module Three: Recovery and Reconstitution
12:05 p.m.	12:30 p.m.	Hot Wash

**All times are approximate*

This page is intentionally left blank.

EXERCISE OVERVIEW

Exercise Name	Violent Extremist Attack Tabletop Exercise (TTX)
Exercise Dates	[Indicate the start and end dates of the exercise]
Scope	This exercise is a TTX planned for [exercise duration] at [exercise location]. Exercise play is limited to [exercise parameters]. This exercise was developed using materials created by the Cybersecurity and Infrastructure Security Agency (CISA) for a CISA Tabletop Exercise Package (CTEP).
Mission Area(s)	Prevention, Protection, Mitigation, Response, and Recovery [Select Appropriate Mission Areas]
Capabilities	Planning; Public Information and Warning; Intelligence and Information Sharing; Interdiction and Disruption; Risk Management for Protection Programs and Activities; Infrastructure Systems; On-Scene Security, Protection, and Law Enforcement; Economic Recovery; Health and Social Services

Objectives	1. Review intelligence and information sharing and dissemination processes in relation to a credible threat to domestic critical infrastructure owners / operators. 2. Assess information sharing capabilities with the public; private sector partners; and federal, state, local, tribal, and territorial government departments and agencies in accordance with applicable plans and procedures. 3. Discuss private sector stakeholders' emergency preparedness plans and response procedures to a multi-stage incident and the coordination of activities under the National Incident Management System (NIMS) with local, state, and federal agencies. 4. Consider using participating organizations' business continuity plans or continuity of operations (COOP) plans to identify best practices in the aftermath of a violent attack on critical infrastructure. 5. [Insert additional exercise objectives as necessary].
Threat or Hazard	Multi-Stage Physical Attack
Scenario	An interactive, discussion-based exercise focused on a violent extremist attack. The scenario consists of three modules: Threat, Incident and Aftermath, and Business Continuity and Recovery.
Sponsor	[Insert the name of the sponsor organization, as well as any grant programs being utilized, if applicable]
Participating Organizations	[Please see Appendix A.]
Point of Contact	[Insert the name, title, agency, address, phone number, and email address of the primary exercise Point of Contact (POC) (e.g., exercise director or exercise sponsor).]

General Information

Exercise Objectives and Capabilities

The following exercise objectives in Table 1 describe the expected outcomes for the exercise. The objectives are linked to capabilities, which are the means to accomplish a mission, function, or objective based on the performance of related tasks, under specified conditions, to target levels of performance. The objectives and aligned capabilities are guided by senior leaders and selected by the Exercise Planning Team (EPT).

Exercise Objectives	Capability
Review intelligence and information sharing and dissemination processes in relation to a credible threat to domestic critical infrastructure owners / operators.	✓ Planning ✓ Intelligence and Information Sharing ✓ Interdiction and Disruption
Assess information sharing capabilities with the public; private sector partners; and federal, state, local, tribal, and territorial government departments and agencies in accordance with applicable plans and procedures.	✓ Planning ✓ Public Information & Warning ✓ Intelligence and Information Sharing
Discuss private sector stakeholders' emergency preparedness plans and response procedures to a multi-stage incident and the coordination of activities under NIMS with local, state, and federal agencies.	✓ Planning ✓ Interdiction and Disruption ✓ Risk Management for Protection Programs and Activities ✓ Infrastructure Systems ✓ On-Scene Security, Protection, and Law Enforcement
Consider using participating organizations' business continuity plans or continuity of operations plans to identify best practices in the aftermath of a violent attack on critical infrastructure.	✓ Planning ✓ Economic Recovery ✓ Health and Social Services
[Insert additional objectives as necessary].	✓ [Insert additional capabilities as necessary]

Table 1. Exercise Objectives and Associated Capabilities

Participant Roles and Responsibilities

The term *participant* encompasses many groups of people, not just those playing in the exercise. Groups of participants involved in the exercise, and their respective roles and responsibilities, are as follows:

- **Players:** Personnel who have an active role in discussing or performing their regular roles and responsibilities during the exercise. Players discuss or initiate actions in response to the simulated emergency.
- **Observers:** Do not directly participate in the exercise. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise.
- **Facilitator:** Provides situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key EPT members also may assist with facilitation as subject matter experts (SMEs) during the exercise.
- **Moderators:** Moderators are responsible for admitting and signing in all participants to the virtual exercise, monitoring the chat area for questions and / or issues, and controlling participant audio.
- **Evaluators:** Are assigned to observe and document the discussion during the exercise, participate in data analysis, and assist with drafting the After-Action Report (AAR).

Exercise Structure

This exercise will be a discussion-based, facilitated exercise. Players will participate in the following three modules:

- Module One: Threat [remove this module for a no-warning exercise]
- Module Two: Incident and Aftermath
- Module Three: Business Continuity and Recovery

Each module begins with a multimedia update that summarizes key events occurring within that time period. After the updates, participants review the situation and engage in discussions of appropriate [insert mission area] issues.

Exercise Guidelines

- This exercise will be held in an open, no-fault environment wherein capabilities, plans, systems, and processes will be evaluated. Varying viewpoints, even disagreements, are expected.
- Respond to the scenario using your knowledge of current plans and capabilities (i.e., you may use only existing assets) and insights derived from your training.
- Decisions are not precedent setting and may not reflect your jurisdiction's/ organization's final position on a given issue. This

exercise is an opportunity to discuss and present multiple options and possible solutions.

- Issue identification is not as valuable as suggestions and recommended actions that could improve [insert mission area] efforts. Problem-solving efforts should be the focus.
- The assumption is that the exercise scenario is plausible, and events occur as they are presented. All players will receive information at the same time.

Exercise Evaluation

Evaluation of the exercise is based on the exercise objectives and aligned core capabilities. Players will be asked to complete a participant feedback form. These documents, coupled with facilitator observations and evaluator notes, will be used to evaluate the exercise and then compiled into the AAR / Improvement Plan (IP).

This page is intentionally left blank.

MODULE ONE: THREAT

Scenario

[Insert Location]

[Insert Month, Day, Year]: [Time]

9 months ago [Alternate Title: "Attack time – 9 months"]

A United States citizen detonates a bomb strapped to his chest on a subway in New York City, killing and injuring dozens of people. Messages left behind indicate that he was inspired by international insurgencies and alleged crimes committed by the United States. Violent extremist organizations worldwide praise his actions.

6 months ago

A man stabs several people leaving a church in Florida with a knife and flees the scene. He is later killed attacking the police officers attempting to apprehend him. A search of his home indicates strong identification with radical philosophies. Violent extremist websites declare that this attack is the latest sign in an uprising of the "faithful" against the "oppressors."

5 months ago

Edgar Smith and Brian Stone are men in their early twenties raised in [insert name of local community]. According to community members, approximately two years ago they allegedly became radicalized and left the United States to fight for a violent extremist organization in another country. They are currently listed on the No-Fly List. Local authorities receive reports that their social media pages are listing them as back in the United States. The Joint Terrorism Task Force (JTTF) is following up on this report.

4 months ago

The U.S. Department of State (State Department) reports that they received a warning and intelligence from the government of another country that there is a heightened risk that violent extremists will attempt a large-scale attack in the United States in the near future. The report suggests that the violent extremists may be planning to arrive by sea and conduct multiple active shooter attacks. The State Department relays the warning to the Department of Homeland Security (DHS), who issues a National Terrorism Advisory System (NTAS) Bulletin and also disseminates the intelligence to state and local officials through fusion centers, sector coordinating council calls, threat briefings, and through the Homeland Security Information Network – Critical Infrastructure (HSIN-CI) postings.

3 months ago

Members of the local community request a permit for holding a rally supporting certain extremist views / actions and condemning United States policies and biased media coverage by journalists. Tensions rise in the community as many object to the upcoming event. Graffiti is found on public buildings denouncing United States policies. A community center, thought by some to shelter those with a tendency to violent extremism, is vandalized with spray-painted slogans criticizing extremism in offensive ways.

10 weeks ago

Many people show up for the rally, chanting slogans and holding signs promoting extremist views. Halfway through the rally, a large group of people arrive to protest the rally and begin heckling and waving signs of their own. The situation rapidly degenerates as groups in each camp begin to throw rocks and other projectiles. With difficulty, law enforcement is able to break up the situation, but 13 people are treated with minor to moderate injuries. In photos of the event appearing in the paper the next day, local officials are able to observe a man, appearing to be Brian Stone, urging on some of the rock throwers.

8 weeks ago

Authorities arrest two men for allegedly planning an attack in Hollywood, Calif. A search of their apartment revealed many guns and homemade explosives. Both men have ties to violent extremist organizations.

5 weeks ago

In the aftermath of the rally, tensions in the community continue to be high. Occasional incidents of vandalism are still occurring. A local source reports to the [insert name of local community] police department that Brian Stone has been in the area several times over the last few weeks, spending a lot of time with young men who are known to be enamored with violent extremist ideas. The source claims that Stone boasted of fighting overseas and has said that he returned to “inspire the faithful.”

4 weeks ago

Federal analysts monitoring a website with known traffic by violent extremists find repeated references to an operation in its planning stages targeting an unmentioned location somewhere in [insert specific region of country, i.e. Deep South, New England].

3 weeks ago

A gun store owner in [insert name of largest city in state] reports to local law enforcement that a man, later identified as Edgar Smith, came in and attempted to buy an AR-15 style rifle. When his information was processed in the National Instant Criminal Background Check System (NICS), his

application to purchase a firearm was denied, after which he became angry and verbally abusive according to the gun store owner. Upon the owner calling the police, Smith left the premises.

The NICS denial was made because Edgar Smith is subject to a court order restraining him from harassing an ex-wife. Information on the NICS denial was transmitted by the Federal Bureau of Investigation (FBI) to the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) in accordance with standard procedures, for potential ATF investigation. It was also distributed to the JTTF.

2 weeks ago

[Insert name of local public venue or government building] reports to the [insert name of local police department] that two men were seen several times loitering around the entrances of the building writing on notepads and taking pictures on each occasion. It was reported to the FBI who passed it to the JTTF for investigation.

10 days ago

A local gun store reports a robbery, and loss of a dozen AR-15 type rifles. Video surveillance shows a group of five masked men entering the store and stealing the weapons and several cases of ammunition.

1 week ago

Two different patrols units in [insert name of local community] report that they have seen people who appear to be following them and taking pictures. One officer attempted to confront the photographer, but he fled the scene.

5 days ago

Federal agencies receive classified information (classified due to the sensitivity of the source) that a domestic attack by violent extremists is imminent. The projected attack is thought to target large venues, possibly involving improvised explosive devices (IEDs) or hostages, but the specifics are uncertain, and the reliability of the information is unclear. As a result, DHS issues a NTAS Elevated Alert.

Discussion Questions

1. If there is identified “suspicious behavior” at your facility, or if you receive information related to potential threats against your facilities and personnel, who do you report this information to?
    a. Are trends of suspicious behaviors tracked across the sector nationwide?

b. Is your organization aware of the "If You See Something, Say Something™" campaign or the National Suspicious Activity Reporting (SAR) Initiative?

c. Would you take any additional measures to monitor for suspicious activities?

d. Example: A patron reports to a member of your staff that he observed a man leave a heavy duffle bag in the entrance area of your facility.

   i. Facility owner: What would you expect your staff to do with that information?

   ii. Facility owner: What would you do when you learned of the report?

   iii. Law Enforcement: If the report is disseminated to 911, a fusion center, or the FBI, what would happen next?

2. What is the process by which your organization would receive intelligence of potential threats? How does your organization receive protective measure recommendations?

   a. What organizations would you communicate with regarding intelligence of threats (e.g., local law enforcement agencies, JTTF, FBI)?

   b. When DHS issues an NTAS bulletin, would you hear about it?

      i. What actions would you take?

   c. Does your organization maintain a relationship with your CISA Protective Security Advisor (PSA)? If so, do you have a rapid means of contacting them?

   d. Does your organization use HSIN-CI?

   e. If the FBI and DHS issue a classified Joint Information Bulletin (JIB), would you receive the information, and how?

      i. What would be done with that information?

   f. Are there established processes to disseminate threat related information internally within your organization? If so, what are those processes?

   g. Are there established processes to share information across the sector with industry partners in other states or regions? If so, what are those processes?

   h. Would you share the threat information that you receive with international industry partners? What would be the benefit, if any?

i. Are there technological barriers, legal considerations, or institutional sensitivities that might affect dissemination of intelligence or threat information?

i. For federal, state, or local agencies, what restrictions regarding access to, and dissemination of, information affect your ability to share information within your organization and with your public and private stakeholders (e.g., Protected Critical Infrastructure Information [PCII], Sensitive But Unclassified (SBU), business confidential)?

ii. How would classified information be shared with local stakeholders?

(1) Are there members of the critical infrastructure sector with clearances?

(2) Would federal authorities issue a tear line product?

(3) What role would the fusion center have?

3. How do you triage the information you receive (formal reporting, rumors, social media, government reports, etc.) for action or further dissemination?

a. Are there specific, essential elements of information you need?

b. What information do you expect from government authorities at this time?

4. If you have evidence of a credible threat to your sector, what actions do you take?

a. Do your emergency response plans (e.g., site security plans, emergency occupancy plans, emergency actions plans, or other appropriate plans) contain protocols for how to operate under a higher threat state?

b. What risk mitigation or protective actions would you implement?

i. Do you coordinate protective measure implementation with any other organization within your sector, or with government entities, such as law enforcement agencies and your PSA?

ii. How are your sector's established protective measures communicated to the government?

iii. How useful are the information bulletins and advisories DHS provides (e.g., a JIB that recommend protective measures?)

iv. Is there a limit on how long you can maintain certain protective actions? If so, how does this factor into your determination of how to implement them?

c. What measures would law enforcement take as the threat escalates against critical infrastructure in the community?

5. What are your key messages concerning a potential threat to your organization?
   a. What do you communicate to your stakeholders?
      i. Who are the key stakeholders or groups (e.g., sectors, agencies, associations) with whom you must communicate?
      ii. Is the message coordinated within your sector? If so, what is the process?
      iii. Are there any advisory organizations that you rely on (e.g. sector councils, regional councils)?
      iv. How would the communication be made (e.g. phone calls, online postings)?
   b. What are you communicating to your employees?
      i. Who in your organization is responsible for addressing employee concerns?
      ii. How is information shared with your employees?
   c. What information would be shared with your community, if any?
      i. What processes are in place to do this?

This page is intentionally left blank.

Module Two: Incident and Aftermath

Scenario: Part One

[Insert Month, Day, Year]

8:11 p.m.

An explosion is heard at [insert name of sports facility, mall, or other major public gathering place]. Reports come in of several people killed or injured at the site. Emergency medical service (EMS), fire, and law enforcement agencies are responding to the scene.

8:14 p.m.

A second explosion is heard on the north side of [insert name of location above]. Initial reports reflect numerous additional casualties.

8:31 p.m.

A white van pulls up to a restaurant in [insert name of city district] and two men jump out, run inside, and open fire on the patrons with AR-15 style weapons. Many people are killed or injured. The assailants run out after about a minute and jump in the van, which speeds away.

Discussion Questions

1. What are the actions of venue personnel in the first five minutes?
    a. How are patrons, spectators, and other people in the area expected to react?
    b. If public safety officials are on-scene, what action do they take in the first five minutes?
    c. Who determines what immediate actions should be taken, and how are these instructions conveyed?
    d. Do facility incident response plans (e.g., site security plans, emergency action plans, emergency response plans, or other appropriate plans) contain protocols for properly responding to the incidents described in the module?
    e. Who maintains decision-making authority when management is not available?
        i. Is this clearly identified in your emergency plans?
    f. Does the facility have notification systems in place to warn employees and patrons both on- and off-site during such an incident?

i. How and when is information shared with patrons?
ii. Is there a way to account for employees (i.e., those who reported for work that day versus those on leave)?
iii. Is there a way to account for patrons?

g. Does the facility have an existing security capability to assist in protecting staff and patrons located in the facility during an emergency?
   i. What resources and assets do you have available to assist in the response?
   ii. If your facility has security personnel, are they armed?
   iii. Are security personnel clearly identifiable to law enforcement?
   iv. Have security personnel been trained to provide guidance to other employees for this type of incident?
   v. What access control measures are or should be in place?
   vi. What are the procedures for safely securing any critical component or operation of the facility?
   vii. What other life safety issues should be considered?
   viii. If doors to critical facility components are locked, how does law enforcement obtain access?

h. What instructions will be given to the employees and patrons (e.g., evacuation, shelter-in-place, lockdown)?
   i. Are employees trained for this type of emergency incident?
   ii. Is emergency contact information made available to the call desk?
   iii. Are procedures in place for sheltering-in-place versus evacuation?
      1. What type of sheltering would be conducted?
      2. What is the process for sheltering in the venue?
      3. What type of evacuation would be conducted?
      4. What is the process for evacuating the venue?
   iv. Is there a safe location identified for people who are evacuating the immediate area?
   v. How would the two explosions impact evacuation routes or shelter-in-place strategies?
   vi. Is there a bomb annex to the plan / instructions?

2. What are first responders' plans and procedures for addressing the first explosion? How do they change when a second report comes in, or when the report of a shooting comes in?
    a. How would your organization hear about what happened?
    b. What actions would your organization take in the first five minutes?
    c. What assets would be sent after the first attack?
    d. How do reports of additional attacks change your response plans?
    e. Would you maintain a reserve of personnel and assets after the first attack? After the second, or third?
    f. Does your locality have mutual aid agreements in place to assist with the response?
    g. Are there protocols in place to address the risk of first responders being targeted in a secondary attack?
    h. How do you respond to reports of a shooting in the context of the entire scenario?
    i. Does your organization have a different response protocol in place for responding to acts of terrorism?
        i. If so, how does it differ?
        ii. If so, what triggers this protocol and who makes the determination that this is an act of terrorism?
    j. In what manner will command and control of the situation be established to adhere to the Incident Command System (ICS)?
        i. How will self-deploying agencies / personnel arriving on-scene be handled?
    k. In addition to responding to the threat, what other services would law enforcement be expected or asked to provide?
3. How are hospitals notified about the number and severity of the wounded?
    a. What procedures are in place to handle a mass casualty incident?
4. Do current venue security plans sufficiently address coordination of emergency response personnel?
    a. In what manner will venue personnel receive information passed to them from public safety agencies, and vice versa?
    b. What does the facility emergency coordinator need to consider (e.g., casualties, evacuation routes, hospitals)?

c. Are any of the facility's incident response plans provided to first responders in preparation for potential incidents?

d. Upon arrival of law enforcement, is there a "go bag" available to them containing desired items such as facility map / floor plans, access swipe cards, elevator keys, etc.?

e. Are there any safety concerns that need to be addressed (e.g., entering restricted or hazardous areas)?

f. How do emergency response personnel access the buildings?

g. Have local law enforcement / first responders participated in exercises and / or training at the facility?

h. Do security personnel and first responders have interoperable radios / communication? Are plans in place for agencies to communicate if they cannot communicate via radio?

i. Are there pre-determined locations of the command post and / or staging area(s)?

j. Is there a process to assist first responders with victim identification?

5. Does your facility maintain security technology that can assist law enforcement in response efforts?

   a. Can security personnel assist in locating victims and assailants via closed-circuit television or similar capabilities?

   b. Are there access control capabilities at the facility to facilitate entry of first responders, prevent entry of visitors or additional employees, and manage contractors on-site?

   c. Does the facility have the ability to remotely control access to critical components or activate / deactivate card readers, including the capability to deactivate a specific card?

   d. Is there appropriate emergency lighting capability at the facility to deal with a nighttime incident?

6. What information are your organizations releasing to the public at this time, if any?

   a. How is public messaging coordinated and who approves the message?

   b. How is media access to the facility and staging areas managed?

7. What systems, processes, technology platforms, and tools are used to officially share information about the status of the response? Do they facilitate information sharing beyond agency, organization, or jurisdictional lines?

8. Are there any procedures in place to monitor news reports of the incident?
    a. What action, if any, would be taken based on new reports?
    b. Are there procedures for monitoring social media reports?
    c. What action, if any, would be taken based on social media reports?

Part One B [Optional]: Second Strike Scenario

8:33 p.m. (Optional)

As fire and EMS personnel triage patients and load them onto ambulances at the site of the first explosion, a man wearing a suicide vest runs toward the incident command post, yells, and detonates an explosive vest. The incident commander is killed, and several members of the command staff are injured. The explosion also kills and injures many of the first responders and the patients that they were assisting, as well as damaging two of the ambulances.

[Optional] Discussion Questions

1. What procedures, if any, do fire and EMS agencies have in place to respond to an attack on their own personnel?
2. If incident command staff is killed or injured, who takes command?
    a. Is this process well known and exercised?
    b. About how long would it take to re-establish a working command post?
    c. What procedures would be considered to ensure the safety of first responders and command staff?
    d. What additional security procedures to ensure responders' safety would be considered that would suspend or slow life-saving operations until fully implemented?
3. How is law enforcement integrated into fire and EMS procedures for responding to an attack?
    a. What resources and actions are required from law enforcement?
    b. Does law enforcement have the available resources to meet those needs, in the context of this scenario?
4. How would this attack impact fire and EMS response?
    a. Would there be a delay in responding to this incident site to secure a perimeter?
    b. Would there be a temporary cessation of response efforts at site on the other side of the building or at the restaurant? If so, when would operations resume?
    c. What precautions would the attack cause fire and EMS agencies to take?
5. Would this attack trigger any additional requests for mutual aid?

Scenario: Part Two

8:50 p.m.

The [insert name of local post office] post office reports that a pair of gunmen entered and fired on people standing in line and at the postal employees before running out of the building. Many people are killed and injured.

9:01 p.m.

Multiple 911 calls come in reporting that several gunmen have entered the [insert name of church, public building, or theater] and are shooting people and taking hostages.

9:22 p.m.

It is confirmed that three or four men carrying rifles and wearing suicide vests have killed several people and captured 20–30 hostages, some of whom are injured to varying degrees.

9:37 p.m.

A restaurant in [insert district of city] reports that a pair of men broke the front window and threw in homemade explosives, which detonated killing and injuring several patrons and employees. They then sped off in a white van.

9:43 p.m.

The hostage takers at [insert name] issued demands to responding law enforcement via loudspeaker, threatening that if law enforcement personnel take any hostile action, the hostages will be killed. They say the kidnapping is in response to crimes the United States has committed internationally and say that they will free the hostages if certain prisoners are released, and if certain foreign policy concessions are made.

9:51 p.m.

A semi-truck driver called 911 and reported that he collided with a speeding white van, and the collision overturned it. He said a man with a gun crawled

out, fired at him, and ran into a nearby [insert name] park. He also said that another man was visible still in the van and appeared to be dead.

Discussion Questions

1. How have events modified the response efforts of fire / rescue agencies?
    a. Do you have the resources to respond immediately to all of these sites?
        i. If not, how are you obtaining the resources?
    b. What is your response to the hostage situation, as the hostage takers still control the scene, and most of the injured?
        i. How would your organization hear about what happened?
        ii. What actions would your organization take in the first five minutes?
        iii. Are medical personnel trained in warm or hot zone entry with responding law enforcement?
2. How would law enforcement agencies address the assailants described in this scenario?
    a. What protocols do you have in place to address a mobile strike team attacking consecutive locations (the team in the white van)?
    b. What are your procedures for force on force contact? Are line officers expected to engage heavily armed assailants, or do departments rely on a tactical response team (i.e. special weapons and tactics [SWAT])?
    c. What specialized equipment do you have for addressing well-armed attackers?[1]
        i. Do your line officers have access to body armor, rifles, tear gas, etc.?
        ii. Does your department have armor plated vehicles or air assets?
        iii. Do you have access to bomb squads?
3. What are your department's plans and procedures for addressing a hostage situation?
    a. Do you have trained negotiators on-staff? Do you access them through a memorandum of understanding (MOU)?
    b. How long will it take negotiators to arrive?

[1] Nothing in this document should be taken to imply the necessity of any particular equipment, or as a recommendation to obtain any such equipment. All resource decisions must be made at the local level, based on local needs and constraints.

c. What are the negotiator's priorities? What would the negotiator be empowered to give in exchange for progress toward those priorities?

d. What resources will negotiators need to effectively complete their mission?

e. What non-law enforcement agencies would need to be at the scene?

4. Which other law enforcement organizations would the local police department be communicating with, and what resources would be requested?

   a. Are the necessary MOUs and memorandums of agreement (MOA) in place for external jurisdictions to assist in response efforts?

   b. At what point would neighboring jurisdictions be alerted, and what assistance would be requested?

   c. At what point would state and federal agencies be alerted to the event?

   d. Do local, county, and state law enforcement have coordinated incident response plans for an active shooter situation? If so, who leads the response?

   e. What information or assistance would state and local officials need from owners / operators during an incident similar to that detailed in this module?

   f. Are there any current standard operating procedures, emergency operating procedures (EOPs), MOAs, and / or MOUs that provide guidance for information sharing regarding events that may have a potential nexus to terrorism?

   g. How and when will the JTTF become involved?

   h. Would there be a request for National Guard involvement?

      i. If so, what role would it play?

      ii. Who would be responsible for requesting the aid, and how would it be activated and coordinated?

5. What non-first responder (fire, EMS, law enforcement) departments / agencies would be needed to support the different scenes?

   a. How are these departments / agencies activated?

   b. How do non first responder departments / agencies integrate into the command structure?

6. What information sharing mechanisms are in place that could be relevant in facilitating response to an incident of this nature?

a. What are your organization's information sharing responsibilities during the response to the incident?
b. Would owners / operators be able to share information to pass pertinent information to prevent potential attacks at other facilities?
c. Would owners / operators be able to relay information to federal, state, and local authorities?
d. Would owners / operators be able to receive information from their federal, state, and local officials?

7. What resources are used to disseminate information?
    a. What notification capabilities (e.g., alerts, email, telecom, text message, special tools) do you use to share information and communicate protective measures implementation?
    b. Are there technological barriers, legal considerations, or institutional sensitivities that might affect information sharing, such as religious customs that prohibit use of electronic communication during specific times?
        i. If so, how will threat-based alerts and notifications be distributed to community members who follow religious customs that prohibit use of electronic communication during specific times?
    c. How are emergency communications handled?
        i. Does dispatch have the resources to address an event of this magnitude?
            1. If not, are there MOUs in place that can provide additional resources?
            2. Are there alternate means of communication?
                a. For responding officials?
                b. For members of the public trying to report emergencies?
        ii. How are communications with state, federal, or mutual aid resources conducted?
            1. Is there interoperable gear available?
            2. Are the training and protocols similar?
            3. Are these communications exercised?
8. What information are your organizations releasing to the public at this time, if any?

a. Who is responsible for this communication?
b. At what point would you consider establishing a Joint Information Center (JIC)?
c. How will owners / operators interact with media representatives and control media access to the facility?
d. Are there procedures in place to manage the media when they arrive?
e. Should additional emergency announcements be made to the public?
f. Will any form of social media be used?
g. How would local law enforcement share information with the community?

9. There have been attacks at several locations. How will personnel accountability and communication be coordinated at each facility?
    a. Who maintains accountability as people are leaving the property?
    b. How do employees leave if the employee parking lot is a crime scene and cannot be accessed?
    c. Is there a protocol for responding to requests for contacting the families of employees during an incident, or addressing their requests for information?

Scenario: Part Three

10:10 p.m.

Police officers responding to [insert name] park, encounter the gunman and exchange small arms fire. The gunman is killed, and one officer is injured by the gunfire.

11:34 p.m.

SWAT teams breach [insert target B] and kill the hostage takers in the process of rescuing the captured civilians. Seven civilians are killed or injured by a detonation and the exchange of gunfire, and 54 people are safely extracted. The SWAT teams reports that the site is secured.

Discussion Questions

1. How does law enforcement determine that a scene is cleared and there are no additional shooters?
    a. Once an all clear is given, how is that information communicated to all personnel sheltered-in-place?
    b. What would your organization do for the next operational period?
    c. For the next week?
    d. How would this incident impact your organization's policies and operations for the foreseeable future?
2. How will law enforcement coordinate the handling of the facility as an active crime scene?
    a. How will law enforcement communicate status with owners / operators?
    b. How will the facility work with this impediment?
    c. Will law enforcement be able to estimate the timeframe required for the facility to be considered a crime scene?
3. How will the locality handle the large increase in deceased persons?
    a. Are there facilities that are available to handle the large number of deceased victims?
    b. Are other assets needed to respond to this increase (e.g. a Disaster Mortuary Response Team [DMORT])?
4. What measures would local law enforcement take at this time to protect local businesses and critical infrastructure (e.g., outreach, increased vigilance, etc.)?

5. What protective security measures will be employed at your organizations following these domestic attacks?
    a. Do you coordinate protective measure implementation with any other organization within your sector, or with government entities, such as law enforcement agencies and your PSA?
    b. How are your sector's established protective measures communicated back to the government?
    c. How useful are the information bulletins and advisories DHS provides (e.g., a JIB) that recommend protective measures?
6. Do your organization's emergency response plans (e.g., site security plans, emergency occupancy plans, emergency actions plans, or other appropriate plans) contain protocol for properly responding to these incidents described in this module? If not, how can that be remedied?

This page is intentionally left blank.

Module Three: Business Continuity and Recovery

Scenario

[Insert Month, Day, Year]

Next Day, 1:00 p.m.

The mayor holds a press conference describing the sorrow of the city at the attack and his admiration of the dedication and effort of first responders. He notes the resolve of the city and lays out his vision for recovery and return to normality.

Next Day, 5:00 p.m.

Law enforcement officials notify the owners of the attacked infrastructure that their properties are considered a crime scene and are likely to remain so for a period of time.

Some period after the attack

Law enforcement officials notify owner / operators of affected infrastructure that forensics has finished and that the areas are released and no longer considered a crime scene.

Discussion Questions

1. How will the ramifications of such an event be addressed in regard to business continuity planning or rapid recovery operations?
    a. Does the facility have a COOP plan or business continuity plan in place?
    b. What are the implications of being unable to open your facility to the public for a period of time?
    c. Does your organization have the ability to relocate to another facility? If so, how long would this take?
    d. How would the loss of personnel impact your operations? What steps would be taken to adjust for, or mitigate this?
    e. How is information communicated with personnel and families during the days following the incident?
    f. Will counseling for employees and family members be available?
    g. Will owners / operators face liability issues from the attack?

2. How will government organizations continue to manage response efforts while beginning long-term recovery processes?
    a. How will employee absences (due to personal / family impacts from the incident) affect response and recovery efforts?
    b. What state and / or federal resources would your organization request? What state and / or federal assistance would your organization require?
    c. What aid would your organization provide to private sector assets or resources?
        i. How are roles and responsibilities delineated?
        ii. What plans or programs outline this aid or assistance?
    d. What private sector assets or resources are available to assist your organization and the overall response effort?
        i. Are pre-arranged agreements in place with private sector organizations to provide resources?
        ii. If so, how are these agreements activated (i.e., what type of coordination and information sharing is required)?
        iii. How will this coordination and information sharing take place?
    e. What non-traditional resources does your organization have access to?
3. What are your organization's interdependencies?
    a. What stakeholders are dependent upon your organization and its services?
    b. Who are the key stakeholders or groups that your organization relies upon to help restore your operations and assets?
    c. What public organizations / resources do private sector organizations rely on to help restore critical infrastructure assets?
    d. What private sector organizations / resources do public sector organizations rely on to help restore mission essential functions?
    e. Do you have contracts / agreements in place with the organizations that control / own these resources / services for priority services in an emergency?
    f. Who are the key mobilizers or champions (either individuals or functional roles) in your organization or community who must be engaged for an effective recovery?
4. What types of information are needed to assist in restoration of your organization's critical infrastructure?

   a. What information would your organization expect to receive? How does your organization expect to receive it and from whom?
   b. What information would your organization expect to provide? How would your organization expect to provide it and to whom?

5. How can owners / operators and government officials prepare to handle the public messaging / media in the aftermath of such an occurrence?
   a. What is your plan for restoring public confidence?
   b. How will you resolve potential misinformation?
   c. How will you respond to and coordinate any requests to comment by the media?

APPENDIX A: EXERCISE PARTICIPANTS

Participating Private Sector Organizations
[Insert private sector participants]

Participating Local Organizations
[Insert local participants]

Participating State Organizations
[Insert state participants]

Participating Federal Organizations
[Insert federal participants]

Other Participating Organizations
[Insert other participants]

Other Participating Organizations

This page is intentionally left blank.

APPENDIX B: RELEVANT PLANS

[Insert excerpts from relevant plans, policies, or procedures to be tested during the exercise.]

This page is intentionally left blank.

APPENDIX C: ACRONYMS

Acronym	Term
AAR	After-Action Report
ATF	Bureau of Alcohol, Tobacco, Firearms, and Explosives
CISA	Cybersecurity and Infrastructure Security Agency
CTEP	CISA Tabletop Exercise
COOP	Continuity of Operations Plans
DHS	Department of Homeland Security
DMORT	Disaster Mortuary Response Team
EMS	Emergency Medical Service
EOP	Emergency Operating Procedure
EPT	Exercise Planning Team
FBI	Federal Bureau of Investigation
HSIN-CI	Homeland Security Information Network – Critical Infrastructure
ICS	Incident Command System
IED	Improvised Explosive Device
IP	Improvement Plan
JIB	Joint Information Bulletin
JIC	Joint Information Center
JTTF	Joint Terrorism Task Force
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NICS	National Instant Criminal Background Check System
NIMS	National Incident Management System
NTAS	National Terrorism Advisory System
PCII	Protected Critical Infrastructure Information
POC	Point of Contact
PSA	Protective Security Advisor
SAR	Suspicious Activity Reporting

Acronym	Term
SBU	Sensitive But Unclassified
SitMan	Situation Manual
SME	Subject Matter Expert
State Department	U.S. Department of State
SWAT	Special Weapons and Tactics
TTX	Tabletop Exercise

CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY